Morecambe Bay

Primary Care Collaborative

Data Protection Policy

Document Reference	POL004
Purpose	The purpose of this document is to ensure that all staff and clinicians working within MBPCC(s) understand their responsibility with regards to DPA and ensure they comply and in the event of a breach ensure the DPO is notified without delay.
Author	Federation Support
Application/Scope	Organisation-wide
Approval Date	17/05/2022
Review Date (N.B: Review dates may alter if any significant changes are made)	17/05/2024
Version	V1.4
Status	APPROVED

Morecambe Bay
Primary Care Collaborative

CONTENTS

1. INTRODUCTION

1.1 Summary

The Data Protection Act 2018 (DPA) requires organisations to have a clear policy for ensuring security of information and to provide individuals with a right of access to a copy of information held about them, encompassing the principles of GDPR.

MBPCC needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

The lawful and proper treatment of personal information by the organisation is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that the organisation treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, loss or destruction of personal information and subject access requests under the Data Protection Act.

For subject access requests refer to the organisation's Subject Access Policy.

1.2 Purpose

MBPCC needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 2018.

We support fully and comply with General Data Protection Regulation (GDPR) principles of

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

1.3 Scope

This policy applies to all MBPCC employees and directors.

From time to time MBPCC may utilise the resources of sub-contractors to deliver contractual obligations. For avoidance of doubt, where a sub-contractor is providing care to patients, as laid out

in the contracts between MBPCC and subcontractors, they are solely responsible for delivery of the regulated activity they are providing, and must ensure all their employees operate under their own policies which must meet the relevant CQC standards. MBPCC will seek assurance from all sub-contractors that suitable policies are in place, and may at their discretion request copies of any relevant policies for review and for verification. In such cases this policy document does not apply.

2. PROCEDURE

2.1 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- comply at all times with the above Data Protection Act principles
- observe all forms of guidance, codes of practice and procedures about the collection and use of personal information
- understand fully the purposes for which the organisation uses personal information
- collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the organisation to meet its service needs or legal requirements
- ensure the information is correctly input into the organisation's systems
- ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required
- ensure that the concept of data minimisation is adhered and that all data anonymisation is undertake in accordance with the Information Commissioner's code of practice (https://ico.org.uk/media/1061/anonymisation-code.pdf)
- on receipt of a request from an individual for information held about them by or on behalf of immediately notify the senior manager
- not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian
- understand that breaches of this Policy may result in disciplinary action, including dismissal

2.2 Organisation Responsibilities

MBPCC will:

- Ensure that there is a named Data Protection Officer with overall responsibility for data protection. Currently this person is the Chief Executive. The Medical Director will take on these responsibilities if the first named individual is absent with illness or on annual leave.
- Maintain its registration with the Information Commissioner's Office
- Ensure that all subject access requests are dealt with as per the organisation's Subject Access Policy.
- Ensure that there is a Caldicott Guardian; this person is the Medical Director.
- Provide training for all staff members who handle personal information
- Provide clear lines of report and supervision for compliance with data protection and also have a system for breach reporting
- Carry out regular checks to monitor and assess new processing of personal data and to ensure the organisation's notification to the Information Commissioner is updated to take account of any changes in processing of personal data

- Develop and maintain DPA procedures to include: roles and responsibilities, notification, subject access, training and compliance testing and use of Data Protection Impact Assessments (see section 6)
- Ensuring that all locations from where services are delivered from display a Privacy Notice in the waiting room explaining to patients the practice policy plus a copy of the Information Commissioners certificate
- Make available a leaflet on Access to Medical Records for the information of patients.
- Take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.
- Undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
- Maintain a system of "Significant Event Reporting" through a fair-blame culture to capture and address incidents which threaten compliance.
- Include DPA issues as part of the organisation's general procedures for the management of Risk.
- Ensure confidentiality clauses are included in all contracts of employment.
- Ensure that all aspects of confidentiality and information security are promoted to all staff.
- Remain committed to the security of patient and staff records.
- Ensure that any personal staff data requested by the CCG or NHS, i.e. age, sexual orientation and religion etc., is not released without the written consent of the staff member

2.3 Lawful Basis for Processing

Patient data will be processed under the following basis

Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and

Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services..."

Staff data will be processed under

Article 6(1)(a) 'the individual has given clear consent to process their personal data for a specific purpose'

Article 9(2)(a) 'the data subject has given explicit consent to the processing of those personal data for one or more specified purposes'

When data can be processed and sharing without consent

Under the GDPR and Data Protection Act 2018 information can be shared without consent if, judged, there is a lawful basis to do so, such as where safety may be at risk. Judgements will need to be based on the facts of the case. Please also refer to MBPCC policies on Safeguarding.

2.4 Data Protection Impact Assessments (DPIA)

A DPIA is a type of risk assessment. It helps to identify and minimise risks relating to personal data processing activities.

The EU General Data Protection Regulation and Data Protection Act 2018 (laws that focus on data privacy for individuals) require us to carry out a DPIA before certain types of processing. This ensures we can mitigate data protection risks.

For instance, if processing personal information is likely to result in a high risk to data subjects' rights and freedoms, we should carry out a DPIA. We should also conduct one when introducing new data processing processes, systems or technologies.

Apart from the legal requirements, DPIAs are a useful way of ensuring the efficiency and cost-effectiveness of the security measures we may implement.

A risk-based approach ensures we do not waste resources attempting to mitigate threats that are unlikely to occur or will have little effect.

Completing DPIAs where necessary support the GDPR's accountability principle, helping us demonstrate compliance with the Regulation, both to the supervisory authority and to other stakeholders.

Guidance and a template for completing a DPIA are available from the Information Commissioner's website at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments.

2.5 Implementation and Monitoring

A copy of this policy will be distributed electronically to each Federation employee and a central record will be held on MBPCC Shared Drive.

MBPCC will undertake annual compliance checks and any shortfalls in compliance will be reported to the Data Protection Officer.

3. DEFINITIONS/GLOSSARY OF TERMS

Abbreviation or Term	Definition
DPA	Data Protect Action
DPIA	Data Protection Impact Assessments
GDPR	General Data Protection Regulation
MBPCC	Morecambe Bay Primary Care Collaborative
CQC	Care Quality Commission

4. CONSULTATION WITH STAFF, PRACTICES AND PATIENTS

Name	Job Title	Date Consulted
Jane Jones	CCG Head of Safeguarding	27/08/2020

5. DISSEMINATION/TRAINING PLAN

Action by	Action Required	Implementation Date
Jo Knight/Boyana Konar	Upload policy to MBPCC website	30/09/2020
Jo Knight	Delete out of date copies and host current copy on Federation G Drive (supporting induction process), updating Policy tracker	30/09/2020
Liz Stedman	Upload to TeamNet	Jan 2021
Liz Stedman	Upload new version to teamnet/Website/Shared Drive	May 2022

6. AMENDMENT HISTORY

Version No.	Date of Issue	Section/Page changed	Description of change	Review Date
V1.0	22/01/2020	N/A	New policy approved	22/01/2022
V1.1	14/07/2020	Not specified	Amendments made on recommendation of CQC	22/01/2022
V1.2	20/09/2020	All	New format	22/01/2022
		2.3 Page 5	Additional information of when data can be shared without consent	
V1.3	19/01/2021	Page 6	Additional Definitions/Glossary of Terms added	
V1.4	17/05/22	Version control	Policy approved	17/05/2024